NRI

Iakyara vol.276

FinTech exposes subcontractor management limitations

Koji Nose

17.January.2018

Nomura Research Institute, Ltd.

Executive Summary

Financial institutions' progressive push into FinTech is enlarging their networks of partners and affiliates and, in turn, increasing their exposure to external risks. Should a financial institution's partner happen to encounter any difficulties that imperil its business continuity, the financial institution itself could be hurt at least reputationally if not financially also. Adeptness at managing all types of subcontractors is a potential determinant of business success or failure.

Koji Nose
General Manager
Financial IT
Risk Management
Department

Stretched supply chains: subcontractor management's limitations

In recent years, financial institutions have been stepping up their oversight of subcontractors at regulatory authorities' behest. Although such oversight now typically extends to every layer of the outsourcing chain, financial institutions still do not monitor their subcontractors and other associates comprehensively enough amid the ongoing FinTech-driven expansion of their partner networks.

One factor behind this deficiency is that financial institutions' oversight of external associates varies depending on the nature of their relationships. Financial institutions are increasingly partnering with external parties that do not technically fit their outsourcing agreements' definition of a subcontractor. Many financial institutions have separate oversight regimes for subcontractors and other associates and implement them through different organizational units. Such differences prevent financial institutions' management from comprehensively comparing external associates.

Another issue is that financial institutions' subcontractor management tends to lack a big-picture perspective because their head-office functions are fragmented into silos. In other words, the purchasing department monitors subcontractors from a financial standpoint; the risk management department, from business-continuity standpoint; the information security department, from the standpoint of information leaks; and so on. Meanwhile, no one is evaluating subcontractors and reporting to management from all such standpoints combined.

An even bigger issue is deficiencies in risk assessment processes. Most financial

institutions are diligent in making sure they comply with standards set by regulators. They conduct appraisals and inquiries using checklists based on safety standards and inspection manuals. In addition to the issue of such checklists' adequacy, another concern is that a front-line organizational unit that utilizes subcontractors and wants to maintain its status quo may not report problems when completing a checklist. Additionally, checklists intended to detect if controls have been implemented are not capable of identifying risks inherent in external associates' operations and functions.

Necessary shift to risk-based management

To rectify such deficiencies in oversight of stretched supply chains, financial institutions need to establish a vendor management office (VMO) or appoint someone to comprehensively manage subcontractors by appropriately evaluating and monitoring them throughout every phase of the lifecycle of the financial institution's relationship with them.

In the US, the Office of the Comptroller of the Currency (OCC) has issued guidance[1)] on financial institutions' third-party relationships, defined to include not only contractual outsourcing relationships but also consensual relationships integral to financial institutions' organizational operations. This definition encompasses alliance partners, affiliates, subsidiaries and joint ventures in addition to subcontractors to which business processes have been outsourced. In response, the US financial institutions have been strengthening their VMO functions to comprehensively manage their third-party relationships. In Japan, a few financial institutions have reportedly set up VMOs within their IT departments. However, it seems that none of those VMOs oversee third-party relationships on an organization-wide basis like in the US.

According to US financial institutions' risk managers interviewed for this article, a newly established VMO's most important task is comprehensive risk assessment of the many third parties with which a typical financial institution has relationships. Through such VMO-led risk assessments, financial institutions classify third parties by risk level into priority-ranked categories.

In the first step of the risk assessment process, individual organizational units concerned with a specific risk such as information security or business continuity assess both inherent and residual risks. The VMO then synthesizes these separate risk assessments into an overall assessment and classifies third parties by risk

NOTE

1) OCC Bulletin 2013-29, Risk Management Guidance on Third-Party Relationships.

level. The US risk managers emphasized the importance of assessing inherent risks by identifying which business processes or functions to be outsourced rather than identifying which third parties to outsource them to. Definitive decisions on which business processes/functions to outsource are made by the heads of the IT, back-office and/or other organizational units that will actually work together with third parties. These managers also determine whether the business processes/functions to be outsourced are "critical activities" as defined by the OCC's guidance. The next step is quantifying residual risk by assessing the effectiveness of the specific (e.g., information security, business continuity) risk controls of the third parties to which the business processes/functions will be outsourced. The VMO then aggregates these risk assessments into a comprehensive assessment for each third party and classifies third parties into 3-5 priority-ranked categories. These categories determine the extent of the VMO's oversight of each third party. For third parties in the highest-priority category, the VMO dispatches its own staff to conduct an on-site assessment before signing a contract with the third party, monitors the status of the third party's controls even after services have commenced and tracks changes in services/risks through dialogue with the third party.

Many Japanese bankers seems to consider the US approach to be overkill. In actuality, however, even a financial institution with 1,000 third-party relationships may only have 5-10 third parties classified in the highest-priority category. Once a financial institution has completed a thorough risk assessment, it can monitor third parties efficiently and effectively. When regulators mandate a risk-based approach to subcontractor management, they may appear at first blush to be imposing a heavier burden on financial institutions but a risk-based approach allows financial institutions to manage subcontractors more efficiently over the long run.

Going forward, Japanese financial institutions must involve their VMOs in FinTech initiatives earlier. Financial institutions have recently been heavily collaborating with FinTech startups in feasibility studies known as proof of concept(PoC) or prototype testing before partnering on new services. If a financial institution discovers that a new service entails a risk it is unwilling to tolerate, it would have to spend time and money on mitigating the risk. Therefore, it is important to conduct a risk assessment with the VMO's participation as early as possible in the PoC/prototype testing phase. Offering new services on a pilot basis within a regulatory sandbox is an effective risk assessment activity that involves feedback from regulatory authorities from a very early stage.

From a risk management standpoint, recent collaborations between financial institutions and FinTech startups appear to have been too focused on minutia or rigor when verifying the implementation status of controls such as API checklists. Instead, financial institutions should place priority on radically revamping subcontractor management best practices through a risk-based approach.

about NRI

Founded in 1965, Nomura Research Institute (NRI) is a leading global provider of system solutions and consulting services with annual sales above $3.7 billion. NRI offers clients holistic support of all aspects of operations from back- to front-office, with NRI's research expertise and innovative solutions as well as understanding of operational challenges faced by financial services firms. The clients include broker-dealers, asset managers, banks and insurance providers. NRI has its offices globally including New York, London, Tokyo, Hong Kong and Singapore, and over 12,000 employees.

For more information, visit http://www.nri.com/global/

Inquiries to : Business Planning & Financial IT Marketing Department
Nomura Research Institute, Ltd.
Otemachi Financial City Grand Cube,
1-9-2 Otemachi, Chiyoda-ku, Tokyo 100-0004, Japan
E-mail : kyara@nri.co.jp

http://www.nri.com/global/opinion/lakyara/index